(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－237186
（P2003－237186A）
(43)公開日　平成15年８月27日(2003.8.27)

(51)Int.Cl.⁷	識別記号	Ｆ Ｉ		テーマコード（参考）
Ｂ４１Ｊ　29/38		Ｂ４１Ｊ　29/38	Ｚ	２Ｃ０６１
5/30		5/30	Ｚ	２Ｃ１８７
29/00		Ｇ０６Ｆ　3/12	Ｋ	５Ｂ０２１
Ｇ０６Ｆ　3/12		Ｇ０６Ｔ　1/00	５００Ｂ	５Ｂ０５７
Ｇ０６Ｔ　1/00	５００	Ｈ０４Ｎ　1/00	Ｂ	５Ｃ０６２

審査請求　未請求　請求項の数20　ＯＬ　（全 12 頁）　最終頁に続く

(21)出願番号　特願2002－41695(P2002－41695)

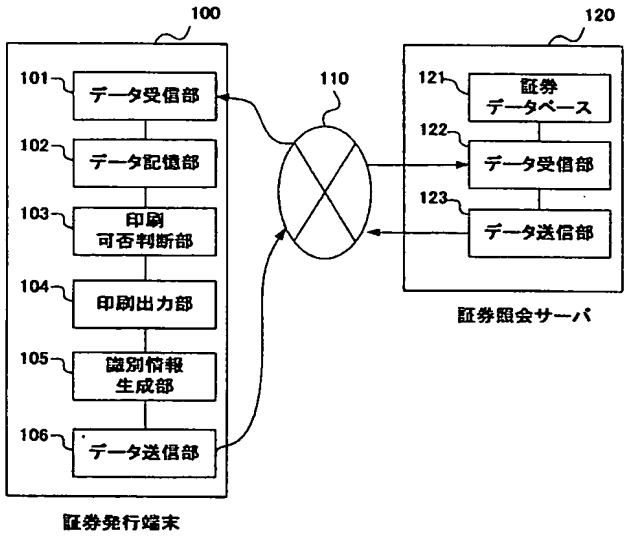
(22)出願日　平成14年２月19日(2002.2.19)

(71)出願人　000000295
沖電気工業株式会社
東京都港区虎ノ門１丁目７番12号
(72)発明者　永重　務
東京都港区虎ノ門１丁目７番12号　沖電気工業株式会社内
(72)発明者　村瀬　嘉史
東京都港区虎ノ門１丁目７番12号　沖電気工業株式会社内
(74)代理人　100095957
弁理士　亀谷　美明　（外２名）

最終頁に続く

(54)【発明の名称】　印刷物発行端末，サーバ，及び印刷物発行方法

(57)【要約】
【課題】　手形，小切手，証券等の印刷物を出力するにあたり，画像データの漏洩，改竄，印刷された証券の複製，改竄等の不正行為を防止する印刷物発行端末，サーバ，及び印刷物発行方法を提供する。
【解決手段】　サーバ１２０へ照会したデータベース１２１にある画像データを，ネットワーク１１０を介して証券発行端末１００のデータ受信部１０１で受信し，これをデータ記憶部１０２が記憶し，印刷可否判断部１０３は印刷済み識別情報が存在すれば印刷不可と，存在しなければ印刷可と判断し，印刷出力部１０４より証券を印刷出力する。また，印刷出力後に識別情報生成部１０５は証券の印刷済み識別情報を生成し，これをネットワーク１１０を介して証券照会サーバ１２０へ送信する。印刷後にデータ記憶部１０２の証券画像データは削除される。



1

【特許請求の範囲】

【請求項１】　ネットワークを介して画像データをサーバから受信するデータ受信部と，前記画像データから印刷済み識別情報を抽出し，前記印刷済み識別情報が存在すれば印刷不可と判断し，前記印刷済み識別情報が存在しなければ印刷可と判断する印刷可否判断部と，前記印刷可否判断部の判断に従い，前記画像データに基づいて印刷物を出力する印刷出力部と，前記印刷物を出力した後に，前記画像データの印刷済み識別情報を生成する識別情報生成部と，前記生成した印刷済み識別情報を，ネットワークを介して前記サーバへ送信するデータ送信部とを有することを特徴とする印刷物発行端末。

【請求項２】　更に，前記サーバから受信した画像データを記憶するデータ記憶部と，前記データ記憶部に記憶された画像データを削除するデータ削除部とを有し，前記印刷出力部は，前記データ記憶部に記憶された画像データに基づいて印刷物を出力するとともに，前記データ削除部は，前記印刷出力部が印刷物を出力した後に，前記データ記憶部に記憶された画像データを削除することを特徴とする請求項１に記載の印刷物発行端末。

【請求項３】　前記識別情報生成部が生成する印刷済み識別情報は，前記画像データから生成された電子署名データを少なくとも含むことを特徴とする請求項１または２のうちのいずれか１項に記載の印刷物発行端末。

【請求項４】　前記電子署名データは，ハッシュ関数を利用して前記画像データから生成されることを特徴とする請求項３に記載の印刷物発行端末。

【請求項５】　前記データ送信部が送信する印刷済み識別情報は，前記画像データの通し番号，及び／または，印刷物発行端末番号を更に含むことを特徴とする請求項３または４のうちのいずれか１項に記載の印刷物発行端末。

【請求項６】　特定の情報を電子透かしとして前記画像データに埋め込む電子透かし埋め込み部を更に有し，前記印刷出力部は，電子透かしを埋め込んだ印刷物を出力することを特徴とする請求項１，２，３，４，または５のうちのいずれか１項に記載の印刷物発行端末。

【請求項７】　前記サーバより受信した，公開鍵暗号方式によって暗号化された画像データを復号する復号部を更に有し，前記暗号化された画像データを前記復号部が復号する際に，ＩＣカード，パスワード，または，バイオメトリクスによって利用者の認証が行われることを特徴とする請求項１，２，３，４，５，または６のうちのいずれか１項に記載の印刷物発行端末。

【請求項８】　前記電子透かしを用いて改竄検出を行う改竄検出部を更に有し，前記改竄検出部が前記画像データの改竄を検出したときに，前記データ送信部は改竄検出情報を前記サーバへ送信することを特徴とする請求項１，２，３，４，５，６または７のうちのいずれか１項に記載の印刷物発行端末。

2

【請求項９】　画像データを保存するデータベースと，印刷物発行端末からの照会情報，及び，前記印刷物発行端末が生成した印刷済み識別情報を，前記印刷物発行端末よりネットワークを介して受信するデータ受信部と，ネットワークを介して，前記印刷物発行端末からの照会情報に応じて前記データベースに保存される画像データと，前記印刷物発行端末により生成された印刷済み識別情報が既に存在している場合に，当該印刷済み識別情報とを，前記印刷物発行端末へ送信するデータ送信部とを有することを特徴とするサーバ。

【請求項１０】　前記データ送信部が送信する印刷済み識別情報は，少なくとも前記画像データから生成された電子署名データを含むことを特徴とする請求項９に記載のサーバ。

【請求項１１】　前記電子署名データは，ハッシュ関数を利用して前記画像データから生成されたことを特徴とする請求項１０に記載のサーバ。

【請求項１２】　前記データ送信部が送信する印刷済み識別情報は，前記画像データの通し番号，及び／または，印刷物発行端末番号を更に含むことを特徴とする請求項１０または１１のうちのいずれか１項に記載のサーバ。

【請求項１３】　特定の情報を電子透かしとして前記画像データに埋め込む電子透かし埋め込み部を更に有し，前記電子透かしを埋め込んだ画像データを前記データ送信部よりネットワークを介して印刷物発行端末に送信する機能を有することを特徴とする請求項９，１０，１１，または１２のうちのいずれか１項に記載のサーバ。

【請求項１４】　前記画像データを公開鍵暗号方式によって暗号化する暗号化部を更に有することを特徴とする請求項９，１０，１１，１２，または１３のうちのいずれか１項に記載のサーバ。

【請求項１５】　前記暗号化部は，認証局が発行する公開鍵証明書が証明する公開鍵を用いることを特徴とする請求項１４に記載のサーバ。

【請求項１６】　ネットワークを介して画像データをサーバから印刷物発行端末へ送信する段階と，前記画像データから印刷済み識別情報を抽出し，前記印刷済み識別情報が存在すれば印刷不可と判断し，前記印刷済み識別情報が存在しなければ印刷可と判断する段階と，前記印刷可否判断に従い，前記画像データに基づいて印刷物を出力する段階と，印刷物を出力した画像データの印刷済み識別情報を生成する段階と，前記生成した印刷済み識別情報を，前記印刷物発行端末からネットワークを介して前記サーバへ送信する段階と，前記印刷済み識別情報を前記サーバのデータベースに保存する段階とを含むことを特徴とする印刷物発行方法。

【請求項１７】　印刷物を出力する段階の後に，前記印刷物発行端末に記憶した画像データを削除する段階を更に含むことを特徴とする請求項１６に記載の印刷物発行

方法。

【請求項１８】　前記画像データの改竄を検出したときに，改竄の検出を出力する段階を更に含むことを特徴とする請求項１６または１７のうちのいずれか１項に記載の印刷物発行方法。

【請求項１９】　前記画像データを送信する段階の前に，特定の情報を電子透かしとして前記画像データに埋め込む段階を更に含むことを特徴とする請求項１６，１７，または１８のうちのいずれか１項に記載の印刷物発行方法。

【請求項２０】　前記画像データを送信する段階の後に，特定の情報を電子透かしとして前記画像データまたは前記印刷物の出力に埋め込む段階を更に含むことを特徴とする請求項１６，１７，１８，または１９のうちのいずれか１項に記載の印刷物発行方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は，印刷物発行端末，サーバ，及び印刷物発行方法に係り，特に，画像データの改竄，漏洩を防止して画像データの原本性を保証するための，ネットワークを介した印刷物発行端末，サーバ，及び印刷物発行方法に関する。

【０００２】

【従来の技術】ネットワークを介して手形や小切手等の証券を発行する従来のシステムは，例えば特開２０００－２９３７３９号公報に開示されている。この公報に記載される証券発行装置は，証券を発行する際に，当該証券の発行データを照会することを許可するための照会識別情報を証券毎に生成する生成手段と，この生成手段により生成された証券毎の照会識別情報と，当該各証券の発行データとを対応付けて記憶する記憶手段と，この記憶手段に記憶された発行データと照会識別情報とを印刷手段により証券に印刷させる印刷制御手段と，を備えたことを特徴とする。上記公報では，このような構成により，証券の所持人は，証券の記載内容を見ることによって固有情報を容易に認識することが可能となり，当該証券の真偽を確認するための照会に必要な情報の入力を迅速且つ適確に行うことができる，としている。

【０００３】上記従来技術のシステムでは，サーバとネットワークで結ばれたクライアントが証券の発行処理を行う際に，サーバが証券の発行データとクライアントから送信された照会識別情報とが一致するかの判別を行って証券発行データの送信可否を判定している。

【０００４】

【発明が解決しようとする課題】しかし，証券会社や銀行などの本店などに備えたサーバから，ネットワークを介して支店などに証券画像データを送信し，支店などにて証券を印刷出力するにあたっては，以下の行為が問題となる。すなわち，支店などに備えた証券発行端末に保存されたデータが，権限のない者に閲覧されたり，持ち出されたり，改竄されたり，複数枚印刷されるなどといった不正行為である。証券画像データの持ち出しは，更に暗号処理方法の解析などに悪用されるおそれもある。上記従来の技術では，このような証券画像の保存データの漏洩，改竄や，印刷された証券の複製，改竄等の不正行為を防止することはできなかった。

【０００５】そこで本発明は，サーバからネットワークを介して画像データを送信し，これを受信する印刷物発行端末により手形，証券，小切手等の画像データを出力するにあたり，画像データの漏洩，改竄や，出力された印刷物の複製，改竄等の不正行為を防止できる印刷物発行端末，サーバ，及び印刷物発行方法を提供することを目的とする。

【０００６】

【課題を解決するための手段】上記目的を達成するための本発明の印刷物発行端末は，ネットワークを介して画像データをサーバから受信するデータ受信部と，画像データから印刷済み識別情報を抽出し，印刷済み識別情報が存在すれば印刷不可と判断し，印刷済み識別情報が存在しなければ印刷可と判断する印刷可否判断部と，印刷可否判断部の判断に従い，画像データに基づいて印刷物を出力する印刷出力部と，印刷物を出力した後に，画像データの印刷済み識別情報を生成する識別情報生成部と，生成した印刷済み識別情報を，ネットワークを介してサーバへ送信するデータ送信部とを有することを特徴とする。

【０００７】このような構成により，出力される印刷物は原本の１通のみとなり，印刷物を複数出力する不正行為を防止することができる。

【０００８】また，上記目的を達成するための本発明の他の印刷物発行端末は，上記構成で更に，サーバから受信した画像データを記憶するデータ記憶部と，データ記憶部に記憶された画像データを削除するデータ削除部とを有し，印刷出力部は，データ記憶部に記憶された画像データに基づいて印刷物を出力するとともに，データ削除部は，印刷出力部が印刷物を出力した後に，データ記憶部に記憶された画像データを削除することを特徴とする。

【０００９】このようにデータ削除部を追加することにより，一端印刷物発行端末内に保存された画像データは，出力後に，または，出力しないと判断された後に不要になれば削除され，画像データの不正な流用や，権限のない者の閲覧，不正な複製，盗難などを防止することができる。画像データの削除が完了したときは，その旨を表示したり，その旨を音声出力したりする機能を付加してもよい。

【００１０】ここで画像データの削除とは，ハードディスクなどの記録メディアから画像データファイルを削除することをいう。単なるファイルインデックス情報の削除だけでなく，その物理的な痕跡を残さずに記録メディ

アから完全に削除することが望ましい。

【００１１】上記識別情報生成部が生成する印刷済み識別情報は，画像データから生成された電子署名データを少なくとも含むことが望ましい。この電子署名データは，ハッシュ関数を利用して画像データから生成することができる。また，データ送信部が送信する印刷済み識別情報は，これに加えて画像データの通し番号，及び／または，印刷物発行端末番号を更に含んでいてもよい。

【００１２】本明細書において「ハッシュ関数」とは，コリジョン（Collision；衝突。例えば，ｘ≠ｙのときＨ（ｘ）＝Ｈ（ｙ）となること。）を見つけることが計算量的に困難な関数をいう。比較的短い固定長の電子署名データは，任意長の証券画像データからこのハッシュ関数を利用して生成され，個々の証券画像データに特有と見なされる情報となる。

【００１３】また，上記目的を達成するための本発明の他の印刷物発行端末は，上記いずれかの構成で更に，特定の情報を電子透かしとして画像データに埋め込む電子透かし埋め込み部を更に有し，印刷出力部は，電子透かしを埋め込んだ印刷物を出力することを特徴とする。このような構成により，出力された印刷物の改竄，不正な複製の発見，防止ができる。

【００１４】ここで「電子透かし」とは，例えば特開平１０－２００７４３号公報等に記載される方法などにより，印刷物の画像中に特定の情報を埋め込む技術をいう。電子透かしとして埋め込まれる特定の情報には，例えば，日時，場所，オペレータ名などを任意に採用すればよい。本発明における電子透かし埋め込みの方法，方式は，特に限定されない。

【００１５】また，上記目的を達成するための本発明の他の印刷物発行端末は，上記いずれかの構成で更に，サーバより受信した公開鍵暗号方式によって暗号化された画像データを復号する復号部を有し，暗号化された画像データを復号部が復号する際に，あらかじめＩＣカード，パスワード，または，バイオメトリクスによってオペレータの認証が行われる。

【００１６】このような構成により，画像データの漏洩，複製，改竄が防止できる。本明細書において「バイオメトリクス」とは，個々人の生体固有の情報を使って認証を行う方式をいう。例えば，指紋や声紋，虹彩を利用する技術などが知られている。

【００１７】本発明において，暗号化の際に使用する公開鍵暗号方式は特に限定されない。また暗号には，例えば，ＲＳＡ暗号，楕円曲線暗号，ＥｌＧａｍａｌ暗号などのアルゴリズムが任意に採用できる。

【００１８】また，上記目的を達成するための本発明の他の印刷物発行端末は，上記いずれかの構成で更に，電子透かしを用いて改竄検出を行う改竄検出部を有し，改竄検出部が画像データの改竄を検出したときに，データ送信部は改竄検出情報をサーバに送信することを特徴とする。

【００１９】このような構成により，画像データの改竄などの不正行為を知ることができ，不正行為に対して早期に対応することができる。

【００２０】上記目的を達成するための本発明のサーバは，画像データを保存するデータベースと，印刷物発行端末からの照会情報，及び，印刷物発行端末が生成した印刷済み識別情報を，印刷物発行端末よりネットワークを介して受信するデータ受信部と，ネットワークを介して，印刷物発行端末からの照会情報に応じてデータベースに保存される画像データと，印刷物発行端末により生成された印刷済み識別情報が既に存在している場合に，当該印刷済み識別情報とを，印刷物発行端末へ送信するデータ送信部とを有することを特徴とする。

【００２１】このような構成により，印刷物発行端末から出力される印刷物は原本の１通のみとなり，印刷物を複数出力する不正行為を防止することができる。

【００２２】上記データ送信部が送信する印刷済み識別情報は，少なくとも画像データから生成された電子署名データを含むことが望ましく，画像データの通し番号，及び／または，印刷物発行端末番号を更に含んでいてもよい。また，この電子署名データは，前述のハッシュ関数を利用して画像データから生成することができる。

【００２３】また，上記目的を達成するための本発明の他のサーバは，上記構成で更に，特定の情報を電子透かしとして画像データに埋め込む電子透かし埋め込み部を有し，電子透かしを埋め込んだ画像データをデータ送信部よりネットワークを介して印刷物発行端末へ送信する機能を有することを特徴とする。

【００２４】このような構成により，印刷可否判断情報や画像データの改竄，不正な複製の発見，防止ができる。ここで画像データに電子透かしで埋め込まれる特定の情報は，例えば，日時，場所，オペレータ名などを任意に採用すればよい。

【００２５】また，上記目的を達成するための本発明の他のサーバは，上記いずれかの構成で更に，画像データを公開鍵暗号方式によって暗号化する暗号化部を有することを特徴とする。また，暗号化に用いる公開鍵は，あらかじめ認証局がオペレータの本人確認を行った上で発行する公開鍵証明書によって，オペレータ本人の公開鍵であることが証明されている公開鍵を用いることを特徴とする。

【００２６】このような構成により，画像データの漏洩，複製，改竄が防止できる。本発明において，暗号化の際に使用する公開鍵暗号方式は特に限定されず，また暗号には，例えば，ＲＳＡ暗号，楕円曲線暗号，ＥｌＧａｍａｌ暗号などのアルゴリズムを任意に採用できる。

【００２７】上記目的を達成するための本発明の印刷物発行方法は，ネットワークを介して画像データをサーバから印刷物発行端末へ送信する段階と，画像データから

印刷済み識別情報を抽出し，印刷済み識別情報が存在すれば印刷済み識別情報の正当性を確認し，正当であると確認できれば印刷不可と判断し，正当であると確認できなければ不正ありと判断してオペレータに通知し，印刷済み識別情報が存在しなければ印刷可と判断する段階と，印刷可否判断に従い，画像データに基づいて印刷物を出力する段階と，印刷物を出力した画像データの印刷済み識別情報を生成する段階と，生成した印刷済み識別情報を，印刷物発行端末からネットワークを介してサーバへ送信する段階と，印刷済み識別情報をサーバのデータベースに保存する段階とを含むことを特徴とする。

【００２８】このような構成により，出力される印刷物は原本の１通のみとなり，印刷物を複数出力する不正行為を防止することができる。

【００２９】また，上記目的を達成するための本発明の他の印刷物発行方法は，上記構成で印刷物を出力する段階の後に，印刷物発行端末に記憶した画像データを削除する段階を更に含むことを特徴とする。

【００３０】このように画像データを削除する段階を追加することにより，一端印刷物発行端末内に保存された画像データは，印刷出力後に，または，印刷しないと判断された後に不要になれば削除され，画像データの不正な流用や権限のない者の閲覧，盗難，不正な複製などを防止することができる。

【００３１】また，上記目的を達成するための本発明の他の印刷物発行方法は，上記いずれかの構成で更に，画像データの改竄を検出したときに，改竄の検出を出力する段階を含むことを特徴とする。

【００３２】ここで出力とは，画像表示，音声出力，印刷出力，サーバへの送信などであり，特に限定されない。このような構成により，不正行為を知ることができ，不正行為に対して早期に対応することができる。

【００３３】また，上記目的を達成するための本発明の他の印刷物発行方法は，上記いずれかの構成で更に，画像データを送信する段階の前に，または，画像データを送信しこれを印刷物発行端末が受信した後に，特定の情報を電子透かしとして画像データに埋め込む段階を含むことを特徴とする。このような構成により，画像データや出力された印刷物の改竄，不正な複製の発見，防止ができる。

【００３４】ここで電子透かしは画像データ中に埋め込んでもよく，また，印刷物のイメージ中に埋め込んでもよい。印刷物のイメージ中に埋め込む方法は，例えば前述の特開平１０－２００７４３号公報等に記載される方法などが利用できる。電子透かしとして埋め込まれる特定の情報は，例えば，日時，場所，オペレータ名などを任意に採用すればよい。本発明における電子透かし埋め込み方法，方式は，特に限定されない。

【００３５】本発明においてネットワークとは，インターネット，専用回線，ＬＡＮ，ＷＡＮ，電話通信網，無線通信網，双方向放送網等を含み，特に限定されない。また，本発明の印刷物発行端末は，唯一のサーバに対応してシステムが構成されていてもよく，また，複数のサーバに対応してシステムが構成されていてもよい。更に，本発明の印刷物発行端末は，単独の端末が存在してシステムが構成されていてもよく，また，複数端末が同時に存在してシステムが構成されていてもよい。

【００３６】

【発明の実施の形態】以下に，本発明のいくつかの実施の形態を，図面を用いて説明する。なお，本明細書及び図面において，実質的に同一の機能構成を有する構成要素については同一の符号を付することにより重複説明を省略する。

【００３７】（第１の実施形態）図１は，本発明の第１の実施形態にかかる証券発行方法を説明する概念図である。証券発行端末１００は，データ受信部１０１，データ記憶部１０２，印刷可否判断部１０３，印刷出力部１０４，識別情報生成部１０５，及びデータ送信部１０６を少なくとも含んで構成される。一方，証券照会サーバ１２０は，証券データベース１２１，データ受信部１２２，及びデータ送信部１２３を少なくとも含んで構成される。証券発行端末１００及び証券照会サーバ１２０は，ネットワーク１１０を介して相互にアクセス可能である。

【００３８】図２は，第１の実施形態の証券発行の手続の流れを示すフローチャートである。まず，ステップＳ１０１で，端末が設置された支店等にてオペレータが証券発行端末１００から証券照会サーバ１２０へ，証券画像データのリストをネットワーク１１０を介して照会する（Ｓ１０１）。この照会をデータ受信部１２２で受けた証券照会サーバ１２０は，証券画像データベース１２１に存在する証券画像データのリストを証券発行端末１００に返す。そして，ステップＳ１０２で，オペレータはこのリストの中から印刷出力したい証券を証券通し番号で指定して選択し，更に証券照会サーバ１２０へ送信する（Ｓ１０２）。

【００３９】次に，ステップＳ１０３で，証券照会サーバ１２０は選択された証券画像データ（図示せず）を，データ送信部１２３からネットワーク１１０を介して証券発行端末１００へ送信する（Ｓ１０３）。証券発行端末１００のデータ受信部１０１はこれを受信し，データ記憶部１０２はこれを記憶する。

【００４０】次に，ステップＳ１０４で，証券発行端末１００の印刷可否判断部１０３は，印刷済み識別情報６００の存在の有無を確認する（Ｓ１０４）。

【００４１】図１１は，印刷済み識別情報６００の構成の一例である。ここでは，印刷済み識別情報６００は，証券画像データ識別番号部６００ａ，電子署名データ部６００ｂ，及び証券発行端末番号部６００ｃの組で構成される。印刷済み識別情報６００の電子署名データ部６

００ｂは，対応する証券画像データからハッシュ関数を利用して生成する。

【００４２】次に，ステップＳ１０５で，もし印刷済み識別情報６００が存在しなければ，ステップＳ１０６で，証券発行端末１００の印刷出力部１０４より，証券を印刷出力する（Ｓ１０５，Ｓ１０６）。

【００４３】次に，ステップＳ１０７で，証券発行端末１００の識別情報生成部１０５が，印刷済み識別情報６００を生成する（Ｓ１０７）。そして，ステップＳ１０８で，証券発行端末１００のデータ送信部１０６が，印刷済み識別情報６００を証券照会サーバ１２０に送信する（Ｓ１０８）。証券照会サーバ１２０のデータ受信部１２２は，印刷済み識別情報６００を受信し，これが証券データベース１２１に保存される。そして手続は終了する。

【００４４】ステップＳ１０５で，もし印刷済み識別情報６００が存在すれば，次にステップＳ１０９で電子署名データ部６００ｂの確認を行う。そして，電子署名が確認できれば手続は終了する。もしステップＳ１０９で電子署名が確認できなければ，次にステップＳ１１０でオペレータに不正ありの通知を行い手続は終了する。

【００４５】このような証券発行方法により，印刷される証券は原本の１通のみとなり，証券を複数印刷する不正行為を防止することができる。

【００４６】（第２の実施形態）図３は，本発明の第２の実施形態にかかる証券発行方法を説明する概念図である。証券発行端末２００は，データ受信部２０１，データ記憶部２０２，印刷可否判断部２０３，印刷出力部２０４，識別情報生成部２０５，データ送信部２０６，及びデータ削除部２０７を少なくとも含んで構成される。一方，証券照会サーバ２２０は，証券データベース２２１，データ受信部２２２，及びデータ送信部２２３を少なくとも含んで構成される。証券発行端末２００及び証券照会サーバ２２０は，ネットワーク２１０を介して相互にアクセス可能である。

【００４７】図４は，第２の実施形態の証券発行の手続の流れを示すフローチャートである。ステップＳ２０１からステップＳ２１０までの流れは，第１の実施形態（図２）の，ステップＳ１０１からステップＳ１１０までの流れと同様であるので説明を省略する。

【００４８】ステップＳ２０８の終了後，または，ステップＳ２０５で肯定分岐のときは，ステップＳ２１１で，証券発行端末２００のデータ削除部２０７が，データ記憶部２０２の証券画像データを削除する（Ｓ２１１）。そして手続は終了する。

【００４９】このようにデータ削除の工程を追加した証券発行方法により，第１の実施形態の効果と同様，印刷される証券は原本の１通のみとなり，証券を複数印刷する不正行為を防止することができる。そして更に，一端証券発行端末内に保存された証券画像データは，印刷出力後に，または，印刷しないと判断された後に不要になれば削除され，証券画像データの不正な流用や権限のない者の閲覧，不正な複製，盗難などを防止することができる。

【００５０】（第３の実施形態）図５は，本発明の第３の実施形態にかかる証券発行方法を説明する概念図である。証券発行端末３００は，データ受信部３０１，データ記憶部３０２，印刷可否判断部３０３，印刷出力部３０４，識別情報生成部３０５，データ送信部３０６，データ削除部３０７，及び改竄検出部３０８を少なくとも含んで構成される。一方，証券照会サーバ３２０は，証券データベース３２１，データ受信部３２２，データ送信部３２３，及び電子透かし埋め込み部３２４を少なくとも含んで構成される。証券発行端末３００及び証券照会サーバ３２０は，ネットワーク３１０を介して相互にアクセス可能である。

【００５１】図６は，第３の実施形態の証券発行の手続の流れを示すフローチャートである。まず，ステップＳ３０１で，端末が設置された支店等にてオペレータが証券発行端末３００から証券照会サーバ３２０へ，証券画像データのリストをネットワーク３１０を介して照会する（Ｓ３０１）。この照会をデータ受信部３２２で受けた証券照会サーバ３２０は，証券画像データベース３２１に存在する証券画像データのリストを証券発行端末３００に返す。そして，ステップＳ３０２で，オペレータはこのリストの中から印刷出力したい証券を証券通し番号で指定して選択し，更に証券照会サーバ３２０へ送信する（Ｓ３０２）。

【００５２】次に，ステップＳ３０３で，証券照会サーバ３２０の電子透かし埋め込み部３２４が，証券画像データに特定のデータを電子透かしによって埋め込む（Ｓ３０３）。

【００５３】次に，ステップＳ３０４で，証券照会サーバ３２０は，選択され，電子透かしが埋め込まれた証券画像データを，データ送信部３２３からネットワーク３１０を介して証券発行端末３００へ送信する（Ｓ３０４）。

【００５４】ステップＳ３０５から終了までの流れは，第２の実施形態（図４）の，ステップＳ２０４から終了までの流れと同様であるので説明を省略する。

【００５５】電子透かし技術を利用すれば，例えば，ある一定以上の解像度の情報を透かし技術によって埋め込んだ印刷物は，複製を行った場合に，一定の解像度以上の情報を正しく読み取ることができない。従って，複製印刷の際に埋め込まれた情報が正しく印刷できず，電子透かしの検出を行った際に埋め込まれた情報を検出できなくなる。これを利用して不正な複製を検出することができる。

【００５６】本実施形態では，複製が行われる際に読み取ることが困難な電子透かし情報を証券画像に埋め込

み，電子透かし情報が正しく印刷されているかどうかを調べることで，不正な複製が行われていないかどうかの判断が可能になる。

【００５７】また，改竄が行なわれた場合は，埋め込まれた情報が改竄によって隠されてしまう。このため，電子透かしの検出を行った際に埋め込まれた情報が検出できなくなる。従って改竄が行われていることが検出できる。

【００５８】このように，第３の実施形態の証券発行方法により，第１の実施形態及び第２の実施形態の効果に加え，印刷出力された証券の改竄，不正な複製の発見，防止ができる効果がある。

【００５９】（第４の実施形態）図７は，本発明の第４の実施形態にかかる証券発行方法を説明する概念図である。証券発行端末４００は，データ受信部４０１，データ記憶部４０２，印刷可否判断部４０３，印刷出力部４０４，識別情報生成部４０５，データ送信部４０６，データ削除部４０７，及び改竄検出部４０８，復号部４０９を少なくとも含んで構成される。一方，証券照会サーバ４２０は，証券データベース４２１，データ受信部４２２，データ送信部４２３，及び暗号化部４２５を少なくとも含んで構成される。証券発行端末４００及び証券照会サーバ４２０は，ネットワーク４１０を介して相互にアクセス可能である。また，証券発行端末４００及び証券照会サーバ４２０から，ネットワーク４１０を介して認証局７００にアクセス可能である。

【００６０】図８は，第４の実施形態の証券発行の手続の流れを示すフローチャートである。ステップＳ４０１，ステップＳ４０２の流れは，第１の実施形態（図２）のステップＳ１０１，ステップＳ１０２の流れと同様であるので説明を省略する。

【００６１】次に，ステップＳ４０３で，証券照会サーバ４２０の暗号化部４２５が，証券画像データを公開鍵暗号方式によって暗号化する（Ｓ４０３）。暗号化に用いる公開鍵は，オペレータ自身が証券照会サーバ４２０に提供するか，または認証局７００より公開鍵証明書を取得することで入手できる。

【００６２】次に，ステップＳ４０４で，証券照会サーバ４２０は，選択され，暗号化された証券画像データを，データ送信部４２３からネットワーク４１０を介して証券発行端末４００へ送信する（Ｓ４０４）。

【００６３】次に，ステップＳ４０５で，証券発行端末４００の復号部４０９が，暗号化されている証券画像データを復号する（Ｓ４０５）。

【００６４】暗号化された証券画像データを復号部４０９が復号する際には，オペレータの認証が行われる。オペレータの認証は，前述したように，ＩＣカード，パスワード，または，バイオメトリクスにより行う。復号に用いる秘密鍵は証券発行端末４００に保存されるか，または，証券発行端末４００のオペレータがＩＣカード内に保持していればよい。対応する公開鍵の提供を認証局７００が行う場合，認証局７００は書面やオンライン利用によるオペレータ本人の確認を行い，公開鍵証明書を発行する。発行された公開鍵証明書には公開鍵が含まれ，証券照会サーバ４２０がネットワーク４１０を介して入手することができる。

【００６５】ステップＳ４０６から終了までの流れは，第２の実施形態（図４）の，ステップＳ２０４から終了までの流れと同様であるので説明を省略する。

【００６６】このような第４の実施形態の構成により，第２の実施形態の効果に加え，証券画像データの漏洩，複製，改竄が防止できる効果がある。

【００６７】（第５の実施形態）図９は，本発明の第５の実施形態にかかる証券発行方法を説明する概念図である。証券発行端末５００は，データ受信部５０１，データ記憶部５０２，印刷可否判断部５０３，印刷出力部５０４，識別情報生成部５０５，データ送信部５０６，データ削除部５０７，及び電子透かし埋め込み部５０９を少なくとも含んで構成される。一方，証券照会サーバ５２０は，証券データベース５２１，データ受信部５２２，及びデータ送信部５２３を少なくとも含んで構成される。証券発行端末５００及び証券照会サーバ５２０は，ネットワーク５１０を介して相互にアクセス可能である。

【００６８】図１０は，第５の実施形態の証券発行の手続の流れを示すフローチャートである。ステップＳ５０１からステップＳ５０５までの流れは，第１の実施形態（図２）のステップＳ１０１からステップＳ１０５までの流れと同様であるので説明を省略する。

【００６９】次に，ステップＳ５０６で，証券発行端末５００の電子透かし埋め込み部５０９が，証券画像データに特定のデータを電子透かしによって埋め込む（Ｓ５０６）。

【００７０】ステップＳ５０７から終了までの流れは，第２の実施形態（図４）の，ステップＳ２０６から終了までの流れと同様であるので説明を省略する。

【００７１】第３の実施形態では，証券画像データへの電子透かしの埋め込みを，証券照会サーバにて行ったが，第５の実施形態では，証券発行端末にて行う。電子透かし埋め込みの効果については第３の実施形態と同様である。従って，第５の実施形態の証券発行方法によれば，第１の実施形態及び第２の実施形態の効果に加え，印刷出力された証券の改竄，不正な複製の発見，防止ができる効果がある。

【００７２】以上，添付図面を参照しながら本発明の証券発行端末，証券照会サーバ，及び証券発行方法の好適な実施形態について説明したが，本発明はこれらの例に限定されない。いわゆる当業者であれば，特許請求の範囲に記載された技術的思想の範疇内において各種の変更例または修正例に想到し得ることは明らかであり，それ

13

らについても当然に本発明の技術的範囲に属するものと了解される。

【００７３】また，本発明は，手形や小切手などの証券に限って説明したが，本発明がこれら以外の原本保証性が要求される書類にも適用できることはいうまでもない。本発明は，証券の印刷に限らず，証券以外の公文書や領収書，一般文書等のあらゆる文書，ロゴマーク，写真等のすべての画像についての印刷にも適用することができる。

【００７４】

【発明の効果】以上説明したように，本発明によれば，証券照会サーバからネットワークを介して証券発行端末により手形や小切手等の証券を印刷出力するにあたり，証券画像の保存データの漏洩，改竄や，印刷された証券の複製，改竄等の不正行為を防止できる証券発行端末，証券照会サーバ，及び証券発行方法が提供できた。

【図面の簡単な説明】

【図１】図１は，第１の実施形態にかかる証券発行方法を説明する概念図である。

【図２】図２は，第１の実施形態の証券発行の手続の流れを示すフローチャートである。

【図３】図３は，第２の実施形態にかかる証券発行方法を説明する概念図である。

【図４】図４は，第２の実施形態の証券発行の手続の流れを示すフローチャートである。

【図５】図５は，第３の実施形態にかかる証券発行方法を説明する概念図である。

【図６】図６は，第３の実施形態の証券発行の手続の流れを示すフローチャートである。

【図７】図７は，第４の実施形態にかかる証券発行方法を説明する概念図である。

【図８】図８は，第４の実施形態の証券発行の手続の流れを示すフローチャートである。

【図９】図９は，第５の実施形態にかかる証券発行方法を説明する概念図である。

【図１０】図１０は，第５の実施形態の証券発行の手続

14

の流れを示すフローチャートである。

【図１１】図１１は，印刷済み識別情報６００の構成の一例である。

【符号の説明】

１００，２００，３００，４００，５００　証券発行端末

１０１，２０１，３０１，４０１，５０１　データ受信部

１０２，２０２，３０２，４０２，５０２　データ記憶部

１０３，２０３，３０３，４０３，５０３　印刷可否判断部

１０４，２０４，３０４，４０５，５０５　印刷出力部

１０５，２０５，３０５，４０５，５０５　識別情報生成部

１０６，２０６，３０６，４０６，５０６　データ送信部

２０７，３０７，４０７，５０７　データ削除部

３０８，４０８　改竄検出部

４０９　復号部

３２４，５０９　電子透かし埋め込み部

１１０，２１０，３１０，４１０，５１０　ネットワーク

１２０，２２０，３２０，４２０，５２０　証券照会サーバ

１２１，２２１，３２１，４２１，５２１　証券データベース

１２２，２２２，３２２，４２２，５２２　データ受信部

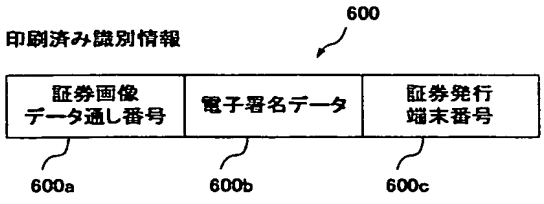
１２３，２２３，３２３，４２３，５２３　データ送信部

４２５　暗号化部

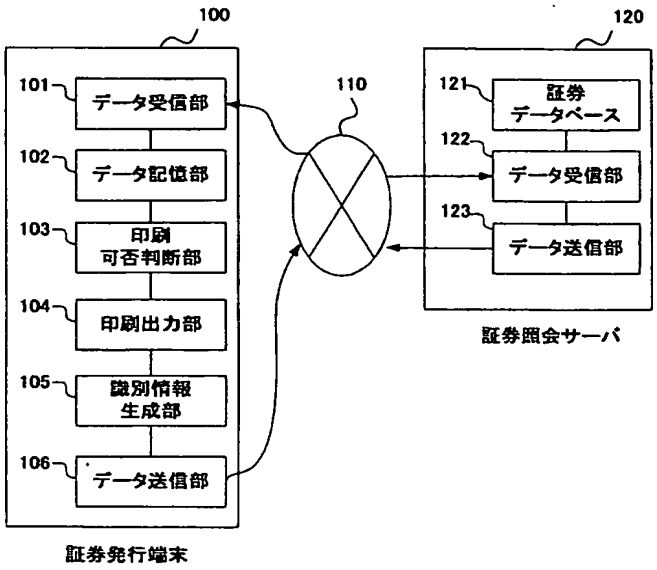
６００　印刷済み識別情報

７００　認証局

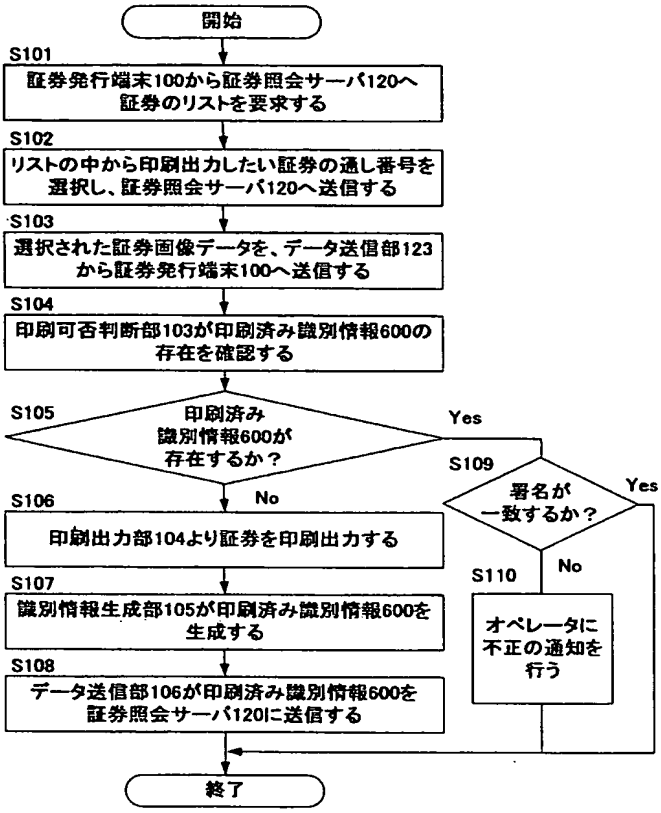
【図１１】



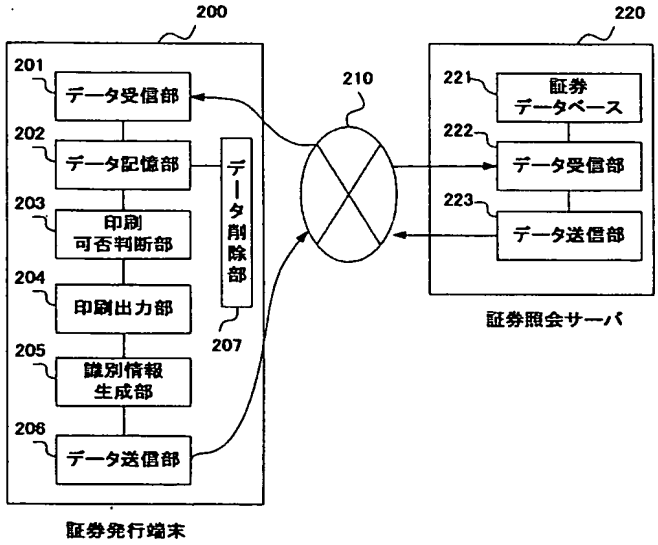
【図１】


100
101
データ受信部
102
データ記憶部
103
印刷
可否判断部
104
印刷出力部
105
識別情報
生成部
106
データ送信部
証券発行端末
110
120
121
証券
データベース
122
データ受信部
123
データ送信部
証券照会サーバ

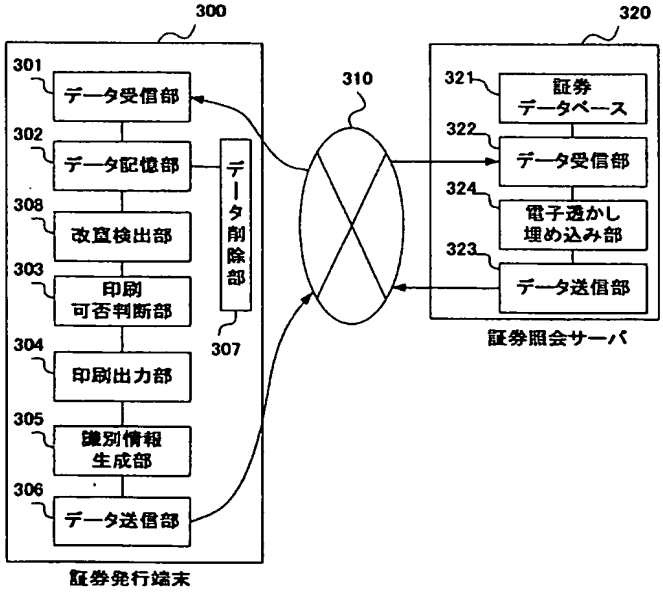
【図２】


開始
S101
証券発行端末100から証券照会サーバ120へ
証券のリストを要求する
S102
リストの中から印刷出力したい証券の通し番号を
選択し、証券照会サーバ120へ送信する
S103
選択された証券画像データを、データ送信部123
から証券発行端末100へ送信する
S104
印刷可否判断部103が印刷済み識別情報600の
存在を確認する
S105
印刷済み
識別情報600が
存在するか？
Yes
No
S109
署名が
一致するか？
Yes
No
S106
印刷出力部104より証券を印刷出力する
S107
識別情報生成部105が印刷済み識別情報600を
生成する
S108
データ送信部106が印刷済み識別情報600を
証券照会サーバ120に送信する
S110
オペレータに
不正の通知を
行う
終了

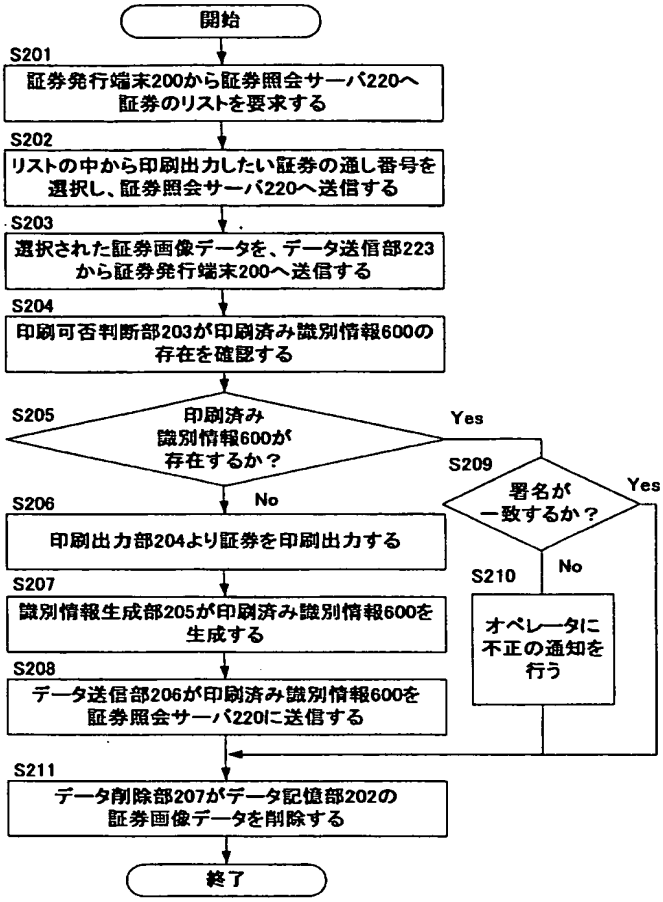
【図３】


200
201
データ受信部
202
データ記憶部
203
印刷
可否判断部
204
印刷出力部
205
識別情報
生成部
206
データ送信部
データ削除部
207
証券発行端末
210
220
221
証券
データベース
222
データ受信部
223
データ送信部
証券照会サーバ

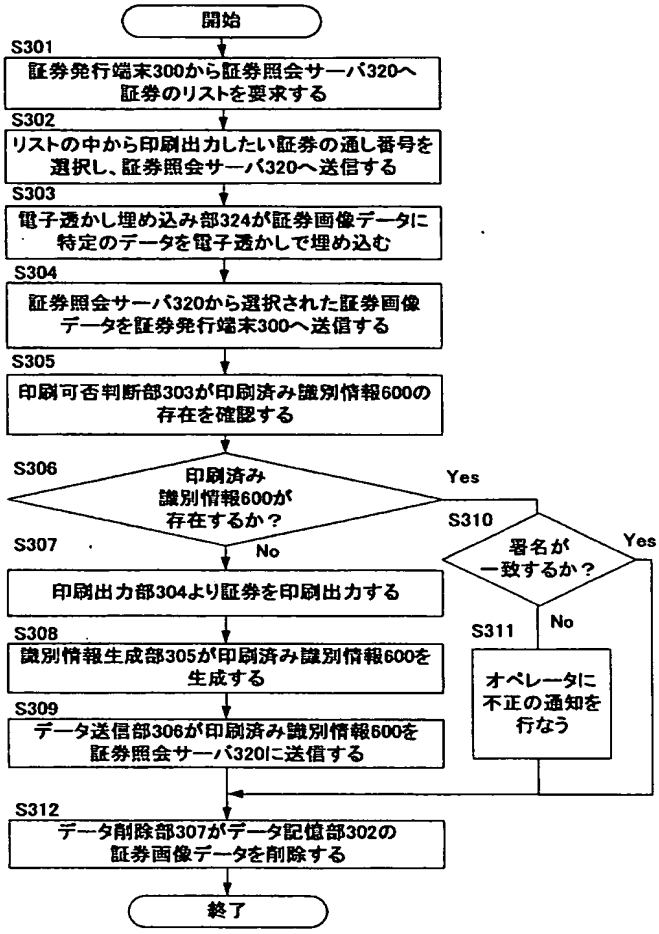
【図５】


300
301
データ受信部
302
データ記憶部
308
改竄検出部
303
印刷
可否判断部
304
印刷出力部
305
識別情報
生成部
306
データ送信部
データ削除部
307
証券発行端末
310
320
321
証券
データベース
322
データ受信部
324
電子透かし
埋め込み部
323
データ送信部
証券照会サーバ

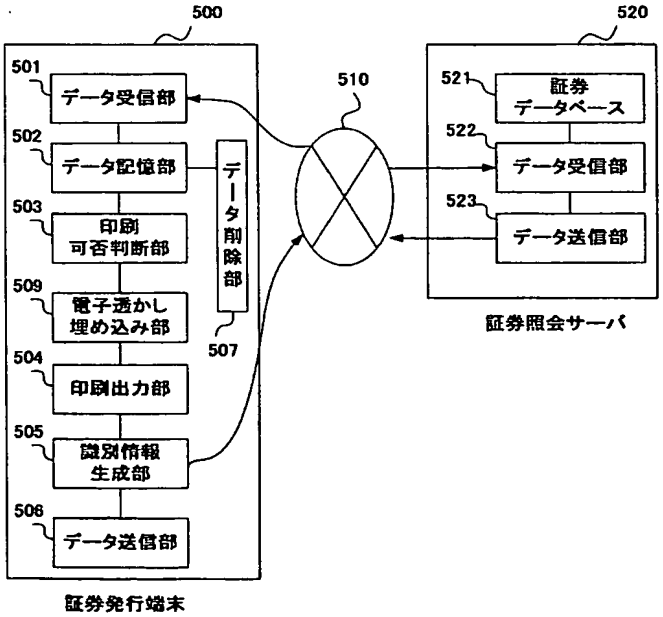
【図４】


開始
S201
証券発行端末200から証券照会サーバ220へ証券のリストを要求する
S202
リストの中から印刷出力したい証券の通し番号を選択し、証券照会サーバ220へ送信する
S203
選択された証券画像データを、データ送信部223から証券発行端末200へ送信する
S204
印刷可否判断部203が印刷済み識別情報600の存在を確認する
S205
印刷済み識別情報600が存在するか？
Yes
No
S209
署名が一致するか？
Yes
No
S206
印刷出力部204より証券を印刷出力する
S210
オペレータに不正の通知を行う
S207
識別情報生成部205が印刷済み識別情報600を生成する
S208
データ送信部206が印刷済み識別情報600を証券照会サーバ220に送信する
S211
データ削除部207がデータ記憶部202の証券画像データを削除する
終了

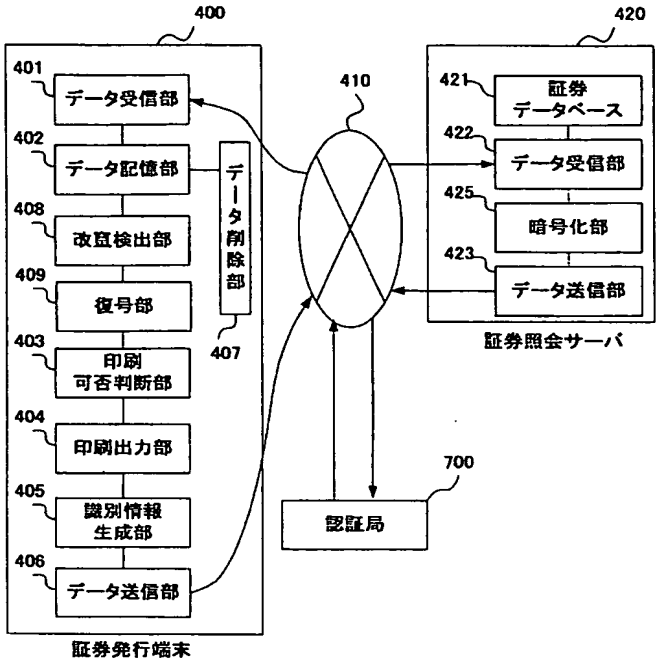
【図６】


開始
S301
証券発行端末300から証券照会サーバ320へ証券のリストを要求する
S302
リストの中から印刷出力したい証券の通し番号を選択し、証券照会サーバ320へ送信する
S303
電子透かし埋め込み部324が証券画像データに特定のデータを電子透かしで埋め込む
S304
証券照会サーバ320から選択された証券画像データを証券発行端末300へ送信する
S305
印刷可否判断部303が印刷済み識別情報600の存在を確認する
S306
印刷済み識別情報600が存在するか？
Yes
No
S310
署名が一致するか？
Yes
No
S307
印刷出力部304より証券を印刷出力する
S311
オペレータに不正の通知を行なう
S308
識別情報生成部305が印刷済み識別情報600を生成する
S309
データ送信部306が印刷済み識別情報600を証券照会サーバ320に送信する
S312
データ削除部307がデータ記憶部302の証券画像データを削除する
終了

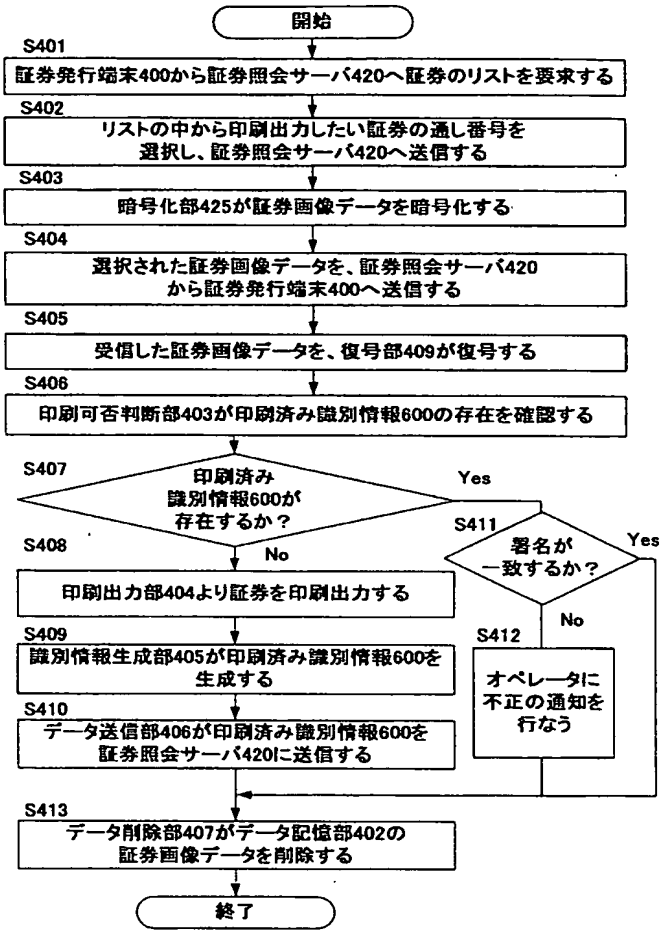
【図９】


500
501
データ受信部
502
データ記憶部
503
印刷可否判断部
509
電子透かし埋め込み部
504
印刷出力部
505
識別情報生成部
506
データ送信部
データ削除部
507
510
520
521
証券データベース
522
データ受信部
523
データ送信部
証券照会サーバ
証券発行端末

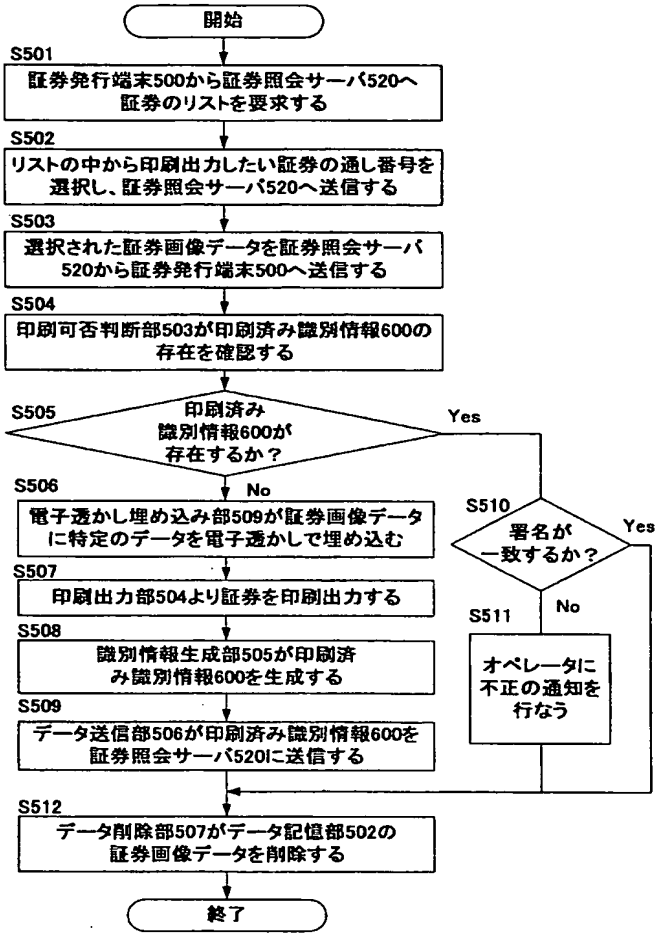
【図７】


400
401
データ受信部
402
データ記憶部
408
改竄検出部
409
復号部
403
印刷
可否判断部
404
印刷出力部
405
識別情報
生成部
406
データ送信部
データ削除部
407
証券発行端末
410
420
421
証券
データベース
422
データ受信部
425
暗号化部
423
データ送信部
証券照会サーバ
700
認証局

【図８】


開始
S401
証券発行端末400から証券照会サーバ420へ証券のリストを要求する
S402
リストの中から印刷出力したい証券の通し番号を
選択し、証券照会サーバ420へ送信する
S403
暗号化部425が証券画像データを暗号化する
S404
選択された証券画像データを、証券照会サーバ420
から証券発行端末400へ送信する
S405
受信した証券画像データを、復号部409が復号する
S406
印刷可否判断部403が印刷済み識別情報600の存在を確認する
S407
印刷済み
識別情報600が
存在するか？
Yes
No
S411
署名が
一致するか？
Yes
No
S408
印刷出力部404より証券を印刷出力する
S412
オペレータに
不正の通知を
行なう
S409
識別情報生成部405が印刷済み識別情報600を
生成する
S410
データ送信部406が印刷済み識別情報600を
証券照会サーバ420に送信する
S413
データ削除部407がデータ記憶部402の
証券画像データを削除する
終了

【図１０】



フロントページの続き

(51) Int.Cl.[7]	識別記号	FI	テーマコード（参考）
Ｈ０４Ｎ　1/00		Ｈ０４Ｎ　1/00	１０７Ｚ　５Ｃ０７６
	１０７	1/387	
1/387		Ｂ４１Ｊ　29/00	Ｚ

(72)発明者　塚本　明利
東京都港区虎ノ門１丁目７番12号　沖電気工業株式会社内

Ｆターム（参考）　2C061 AP01 CL08 HH01 HH03 HJ06 HK11 HN05 HN23
2C187 AE07 AE20 BF19 BF26 BF34 GC09 GD02 GD06
5B021 AA11 NN18 NN19
5B057 AA11 CB19 CE08
5C062 AA02 AA05 AA29 AB38 AC21 AC41 AC42 AC43 AC58 AF00 BA00
5C076 AA14 BA06